ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 24, Number 2, Spring 1994

# ALGEBRAIC DYNAMICS OF POLYNOMIAL MAPS ON THE ALGEBRAIC CLOSURE OF A FINITE FIELD, I

ANJULA BATRA AND PATRICK MORTON

ABSTRACT. We study the dynamics of a polynomial map $\sigma(x)$ on the algebraic closure of the finite field $\mathbf{F}_q$ by defining an induced map $\hat{\sigma}$ on the irreducible polynomials over $\mathbf{F}_q$: $\hat{\sigma}(f) = g$ if $f(x)$ divides $g(\sigma(x))$. We show in general that $\hat{\sigma}$ has infinitely many fixed points. For the special maps $\sigma(x) = x^q + ax$, with $a \neq 0$ in $\mathbf{F}_q$, we also compute the degrees of the periodic points of $\sigma$ over $\mathbf{F}_q$ and show that $\hat{\sigma}$ has an infinite number of periodic points which are not fixed points.

**1. Introduction.** In this paper and its sequel we study the dynamics of special polynomial maps on the algebraic closure $\hat{\mathbf{F}}_q$ of the finite field $\mathbf{F}_q$ having $q$ elements. We hope to show that interesting phenomena arise when questions that are typical in the study of classical "analytical" dynamical systems are studied in an algebraic context. (Compare [**11, 16, 14, 15**] in the references at the end of the paper. See also [**9, 5**] for a discussion of other connections between dynamical systems and number theory.)

As our starting point we will take a polynomial $\sigma(x)$ defined over the finite field $\mathbf{F}_q$, and, inspired by Vivaldi [**15**], we make the following definition.

Let $G_\sigma$ be the directed graph whose vertices are all the monic irreducible polynomials over $\mathbf{F}_q$, and where $g \to f$ is an edge in this graph if and only if $g(x)$ divides $f(\sigma(x))$. Equivalently, $g \to f$ if $\alpha$ is a root of $g$ and $\sigma(\alpha)$ has minimal polynomial $f$.

For a given $g$ there is exactly one $f$ for which $g \to f$ (see Vivaldi [**15**] and Section 3), so that $\sigma$ induces a well-defined mapping $\hat{\sigma}$ on

The second author was supported by a Brachman-Hoffman grant from Wellesley College, and both authors were supported by NSF Grant DMS-9200575, during the period in which this article was written.
Received by the editors on May 13, 1993, and in revised form on October 12, 1993.
1991 AMS *Subject Classification.* 12E20, 5C20.

irreducible polynomials. Thus, $f = \hat{\sigma}(g)$ if $\sigma$ maps roots of $g$ to roots of $f$, and $f(x)$ divides $f(\sigma(x))$ if and only if $f$ is a fixed point of $\hat{\sigma}$.

Our first result concerning this graph and induced map is the following (see Theorem 3.6).

**Theorem A.** *For any nonconstant polynomial $\sigma(x)$ in $\mathbf{F}_q[x]$, the induced map $\hat{\sigma}$ has an infinite number of fixed points. Equivalently, $G_\sigma$ has infinitely many cycles of length 1. In particular, $G_\sigma$ has infinitely many connected components.*

Moreover, the map $\hat{\sigma}$, or equivalently, the graph $G_\sigma$, gives a convenient vehicle for describing the dynamics of a polynomial map $\sigma$ on the whole algebraic closure of $\mathbf{F}_q$.

In this paper and the sequel we will study the maps $\sigma(x) = x^q + ax$ in detail, where $a \neq 0$ is an element of the finite field $\mathbf{F}_q$. (Many of the methods will also apply to any additive polynomial over $\mathbf{F}_q$, i.e., a polynomial of the form $\sigma(x) = \sum_i a_i x^{q^i}$; see [**10**], where they are referred to as "linearized" polynomials.)

For these maps we show that the induced map $\hat{\sigma}$ also has infinitely many periodic points which are *not* fixed points. This is one expression of the fact that these maps have fundamentally different dynamics from the Frobenius map $\phi(x) = x^q$. In order to prove this, and to prepare for the analysis in the sequel of the structure of $G_\sigma$, we give a detailed investigation of the degrees of the $m$-th order periodic points of $\sigma$ as they depend on $m$. Among the results we prove are the following.

Let $\Phi_{m,\sigma}(x)$ be the polynomial defined by

$$\Phi_{m,\sigma}(x) = \prod_{d|m} (\sigma^d(x) - x)^{\mu(m/d)}, \tag{1}$$

where $\mu$ is the Möbius $\mu$-function (see [**11, 16**]). From [**11**] all the periodic points of $\sigma$ of primitive period $m$ (i.e., minimal period $m$) are roots of $\Phi_{m,\sigma}(x)$. To describe how $\Phi_{m,\sigma}(x)$ factors when $\sigma(x) = x^q + ax$, we let $P_d$ be the set of primitive divisors of $q^d - 1$: these are the positive integers which divide $q^d - 1$ but do not divide $q^k - 1$ for $1 \leq k < d$.

**Theorem B.** *Let* $\sigma(x) = x^q + ax$*, where* $a \in \mathbf{F}_q$*,* $a \neq 0$*, If* $(m, q) = 1$ *and* $d$ *is the order of* $q$ *modulo* $m$*, then the degrees of the irreducible factors of* $\Phi_{m,\sigma}(x)$ *are all primitive divisors of* $n = q^d - 1$*. Moreover, the set of irreducible polynomials over* $\mathbf{F}_q$ *whose degrees are in the set* $P_d$ *coincides with the set of irreducible factors of* $\Phi_{m,\sigma}(x)$ *and of* $\Phi_{m,\sigma}(\sigma(x))$ *for* $m$ *in* $P_d$*.*

If the level of an irreducible polynomial $f$ in $G_\sigma$ is defined to be the least nonnegative integer $k$ for which $\hat{\sigma}^k(f)$ lies in a cycle, then the last assertion of this theorem implies that all polynomials with degree prime to $q$ lie either at level 0 or at level 1 in $G_\sigma$ (see the diagrams in Section 3).

Related to the last theorem is the following result (see Section 6).

**Reciprocity theorem.** *For any integers* $m$ *and* $n$ *prime to* $q$*, and any* $a \neq 0$ *in* $\mathbf{F}_q$*, the number of distinct roots of* $\Phi_{m,x^q+ax}(x)$ *of degree* $n$ *equals the number of distinct roots of* $\Phi_{n,x^q-ax}(x)$ *of degree* $m$*.*

In the special case $q = 2$ we also have the following curious result (see Section 5).

**Theorem C.** *If* $p$ *is prime, then all the irreducible factors of* $\Phi_{p,x^2+x}(x)$ *over* $\mathbf{F}_2$ *have degree* $p$ *if and only if* $p$ *is a* Mersenne *prime, i.e.,* $p = 2^l - 1$ *for some prime* $l$*.*

For the map $\sigma(x) = x^2 + x$ over $\mathbf{F}_2$, Theorems B and C and the reciprocity theorem imply:

**Theorem D.** *The induced map* $\hat{\sigma}$ *of* $\sigma(x) = x^2 + x$ *(over* $\mathbf{F}_2$*) has infinitely many odd periods which are relatively prime in pairs.*

There is a similar (but weaker) result for arbitrary maps of the form $\sigma(x) = x^q + ax$ (see Theorem 6.5 and its corollaries).

The results of this paper concern the nature of the irreducible polynomials in cycles in the graph $G_\sigma$. This is because an irreducible polynomial $f$ belongs to a cycle in $G_\sigma$ if and only if $f$ divides $\Phi_{m,\sigma}(x)$ for some $m$ (see Section 3). In the sequel to this paper we will study the dynamics of these maps further by investigating the detailed structure of higher levels of the associated graphs $G_\sigma$. The Galois theory will play an important role in showing that many of the connected components of $G_\sigma$ are isomorphic to each other.

We note that the polynomials $\Phi_{m,\sigma}(x)$, where $\sigma(x) = x^q + ax$, are specializations of the corresponding polynomials $\Phi_{m,x^q+Tx}(x)$ over the rational function field $\mathbf{F}_q(T)$ (see [**11**, Theorem 3]). The latter polynomials are products of analogues of cyclotomic polynomials which occur in connection with the Carlitz module (see [**4**] and [**8**]). Thus, some of the results proved here are related to classfield theory over $\mathbf{F}_q(T)$ and could be proved by investigating the splitting of the prime divisor $T - a$ of $\mathbf{F}_q(T)$ in the appropriate abelian extensions of $\mathbf{F}_q(T)$. In this paper we have chosen a more direct approach which avoids this connection with classfield theory. On the other hand, we will use the Carlitz module in a later paper to get more detailed information about the lengths of the cycles in $G_\sigma$. The results proved in these papers form part of the foundation for a study of the algebraic number theory of the splitting fields over $\mathbf{Q}$ of the polynomials $\Phi_{m,\sigma}(x)$, with $\sigma(x) = x^q + ax$ and $a$ in $\mathbf{Q}$.

**2. Background and the dynamics of the Frobenius map.** We start by recalling some elementary definitions from dynamical systems (see [**1, 6, 11**]).

A periodic point of a polynomial map $\sigma$ over a field $\kappa$ is an element $\alpha$ of the algebraic closure $\hat{\kappa}$ of $\kappa$ for which $\sigma^m(\alpha) = \alpha$ for some integer $m$, where $\sigma^m$ is the $m$-th iterate of $\sigma$:

$$\sigma^m(x) = \underbrace{\sigma(\sigma(\cdots\sigma}_{m}(x))).$$

We will say $\alpha$ has *order* $m$ (or *period* $m$) if $\sigma^m(\alpha) = \alpha$ and *primitive order* $m$ (or *primitive period* $m$) if $\sigma^k(\alpha) \neq \alpha$ for $k < m$. Thus, the periodic points of $\sigma$ of order $m$ are all the roots of $\sigma^m(x) - x = 0$. An element $\alpha$ of $\hat{\kappa}$ is pre-periodic if $\sigma^{k+m}(\alpha) = \sigma^k(\alpha)$, for some $k$ and $m$, that is, if $\sigma^k(\alpha)$ is a periodic point. The *forward orbit* of any number $\alpha$ is just the set of iterated images of $\alpha$ under $\sigma$:

$$\text{forward orbit of } \alpha = \{\alpha, \sigma(\alpha), \sigma^2(\alpha), \dots, \sigma^k(\alpha), \dots\}.$$

In particular, $\alpha$ is pre-periodic if and only if its forward orbit is finite. If $\alpha$ is periodic of primitive order $m$, its forward orbit consists of exactly $m$ distinct elements, and each of the elements of this orbit are periodic points having primitive order $m$ (see [**11**, Lemma 1]).

**Lemma 2.1.** *If $\sigma$ is a polynomial map defined over $\mathbf{F}_q$, every element of $\hat{\mathbf{F}}_q$ is a* pre-periodic point *with respect to $\sigma$.*

*Proof.* Let $\alpha$ be an element of $\hat{\mathbf{F}}_q$. Since $\sigma$ maps the finite set $\mathbf{F}_q(\alpha)$ into itself, the forward orbit of $\alpha$ is obviously finite and $\alpha$ is pre-periodic. $\square$

Hence, to understand the dynamics of $\sigma$ on $\hat{\mathbf{F}}_q$, we need only study periodic and pre-periodic points.

In order to isolate the periodic points of *primitive* order $m$, we introduce the polynomial $\Phi_{m,\sigma}(x)$ defined by (1). In terms of $\Phi_{m,\sigma}(x)$ we have the factorization

$$\sigma^m(x) - x = \prod_{d|m} \Phi_{d,\sigma}(x) \tag{2}$$

(see [**11, 16**]). In [**11**] it is shown that $\Phi_{m,\sigma}(x)$ is a polynomial whenever $\sigma$ is, even when $\sigma^m(x) - x$ has multiple roots. This is important since there will often be multiple roots for the maps we are considering. The polynomial $\Phi_{m,\sigma}(x)$ also has the property that $\Phi_{m,\sigma}(x)|\Phi_{m,\sigma}(\sigma(x))$, which implies that the map $\sigma$ is a permutation on the roots of $\Phi_{m,\sigma}(x)$.

Equating degrees in (1) gives the formula

$$\deg \Phi_{m,\sigma}(x) = \sum_{d|m} \mu\left(\frac{m}{d}\right)(\deg \sigma)^d. \tag{3}$$

All the periodic points of $\sigma$ of primitive order $m$ must be roots of $\Phi_{m,\sigma}(x)$ by (1), though $\Phi_{m,\sigma}(x)$ can also have roots which are nonprimitive. By the results of [**11**] (see Theorem 1c) any such nonprimitive roots must be multiple roots of $\Phi_{m,\sigma}(x)$ whenever $m$ is not divisible by the characteristic of the groundfield $\kappa$.

As an example, consider the map $\phi(x) = x^q$ over $\mathbf{F}_q$. The iterates of $\phi$ are $\phi^m(x) = x^{q^m}$, and so the periodic points of $\phi$ of order $m$ are just the elements of the field $\mathbf{F}_{q^m}$. The elements of primitive period $m$ are the elements of $\mathbf{F}_{q^m}$ which are fixed by $\phi^m$ but by no smaller power of $\phi$, and so these are exactly the elements of degree $m$ over $\mathbf{F}_q$. Since $\phi^m(x) - x$ has distinct roots, it follows easily from (1) and (2) that $\Phi_{m,\phi}(x)$ is the product of all the irreducible polynomials over $\mathbf{F}_q$ of degree $m$. From (3) now follows the well-known fact that the number $N(m, \mathbf{F}_q)$ of irreducible polynomials of degree $m$ over $\mathbf{F}_q$ is given by

$$N(m, \mathbf{F}_q) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{m}{d}\right) q^d \tag{4}$$

(see [**10**]).

Note that every element of $\hat{\mathbf{F}}_q$ is a periodic point of $\phi$, and the elements of the orbit containing $\alpha$ are just the conjugates of $\alpha$ over $\hat{\mathbf{F}}_q$. Thus, the dynamics of the map $\phi$ are particularly simple and coincide with the Galois theory of $\hat{\mathbf{F}}_q$.

**3. The graph $G_\sigma$.** The second main tool we will use for studying the dynamics of a map $\sigma$ is a graph $G_\sigma$ defined as follows. The vertices of the *directed graph* $G_\sigma$, defined over a field $\kappa$, will be all the monic irreducible polynomials over $\kappa$. For two vertices $f$ and $g$ in this graph, we will have

$$g \to f \qquad \text{if and only if} \qquad g(x) \mid f(\sigma(x)).$$

The reason for this definition is made clear in the following lemma, which is valid over any field $\kappa$.

**Lemma 3.1.** *Let $\sigma(x)$ be a polynomial with coefficients in a field $\kappa$. If $f(x)$ and $g(x)$ are irreducible over $\kappa$, then $g(x)$ divides $f(\sigma(x))$ if and only if $\sigma$ maps roots of $g$ to roots of $f$. In particular, if $g$ is a vertex in $G_\sigma$, then there is exactly one vertex $f$ for which $g \to f$.*

*Proof.* Assume first that $g(x)$ divides $f(\sigma(x))$. From $f(\sigma(x)) = g(x)h(x)$ it is clear that $g(\alpha) = 0$ implies $f(\sigma(\alpha)) = 0$. Thus, $\sigma$ maps roots of $g$ to roots of $f$. If, conversely, $f(\sigma(\alpha)) = 0$ for a root $\alpha$ of $g$, then $f(\sigma(x))$ is divisible by the minimal polynomial of $\alpha$, which is $g(x)$, and $\sigma(\alpha)$ is a root of $f$ for *every* root $\alpha$ of $g$. This implies the last assertion. Alternatively, if $f_1(x)$ and $f_2(x)$ are monic, irreducible and distinct, then an appropriate linear combination of $f_1$ and $f_2$ equals 1, and substituting $\sigma(x)$ shows that $(f_1(\sigma(x)), f_2(\sigma(x))) = 1$ also. □

The assertions of Lemma 3.1 show that $\sigma$ induces a mapping $\hat{\sigma}$ on irreducible polynomials over $\kappa$, where we write $\hat{\sigma}(g) = f$ if $g \to f$. We can use the graph $G_\sigma$ to study the dynamics of $\sigma$ on the algebraic closure $\hat{\kappa}$. This is a slight extension of the idea considered by Vivaldi in [**15**], where irreducible polynomials are used to study the dynamics of polynomial maps.

**Lemma 3.2** (see [**15**]). *Let $\sigma(x)$ be a polynomial with coefficients in a field $\kappa$. If $g \to f$ in $G_\sigma$, then* $\deg f$ *divides* $\deg g$.

*Proof.* By the previous lemma, $g \to f$ means that $\sigma$ maps roots of $g$ to roots of $f$. Let $\alpha$ be a root of $g$. Then $\kappa(\sigma(\alpha))$ is a subfield of $\kappa(\alpha)$, and the lemma follows from the tower law of field theory by virtue of

$$[\kappa(\alpha) : \kappa] = \deg g \quad \text{and} \quad [\kappa(\sigma(\alpha)) : \kappa] = \deg f. \qquad \square$$

As an example, note that the graph $G_{x^q}$ over $\mathbf{F}_q$ is totally disconnected in the sense that the only vertex connected to a vertex $f$ is $f$ itself. This follows from

$$f(\sigma(x)) = f(x^q) = f(x)^q \qquad (\text{over } \mathbf{F}_q).$$

Thus, $G_{x^q}$ can be considered the "trivial graph" in this context.

The following diagrams show pieces of several of the connected components of the graph $G_{x^2+x}$ over $\mathbf{F}_2$. In this graph the notation $(d_1, d_2, \ldots, d_n)$ represents the polynomial

$$x^{d_1} + x^{d_2} + \cdots + x^{d_n}, \qquad \text{with } d_1 > d_2 > \cdots > d_n.$$

As we will show, $G_{x^2+x}$ has an infinite number of connected components, many of which are isomorphic to the connected component of the polynomial $x$.

In the following three lemmas we characterize the cycles in the graph $G_\sigma$. All three lemmas are valid over an arbitrary field $\kappa$.

**Lemma 3.3.** *If $f$ is a vertex in $G_\sigma$ which belongs to a cycle, then $f$ divides $\Phi_{m,\sigma}(x)$ for some $m$.*

*Proof.* To prove the first statement, let $\alpha$ be a root of $f(x)$. Since $f$ belongs to a cycle, there is some path in $G_\sigma$ that begins and ends with $f$. Let such a cycle, say

$$f \to g_1 \to \cdots \to g_k \to g_{k+1} \to \cdots \to f,$$

have length $n$, so that $g_n = f$. By definition, we have that $g_k(x) \mid g_{k+1}(\sigma(x))$ for any consecutive vertices $g_k$ and $g_{k+1}$ in the cycle, so that $f(x) \mid g_k(\sigma^k(x))$ for all $k$. Hence, $f(x) \mid f(\sigma^n(x))$, and Lemma 3.1 implies that $\sigma^n$ maps roots of $f$ to roots of $f$. Thus, the orbit of $\alpha$ under $\sigma^n$ is finite and $\sigma^{kn}(\alpha)$ is a periodic point of $\sigma^n$ for some $k$. But $\sigma^{kn}(\alpha)$ is a root of the irreducible polynomial $f(x)$, which must therefore be a factor of $\sigma^m(x) - x$ for some multiple $m$ of $n$. Consequently, $f$ divides $\Phi_{m,\sigma}(x)$ for some $m$, by (2). □

To prove the converse of Lemma 3.3 we need the next lemma, which depends on the fact that the orbit of a periodic point consists entirely of periodic points with the same primitive period.

**Lemma 3.4** (see [**11**, Lemma 9]). *If $f(x) \mid \Phi_{m,\sigma}(x)$, where $f(x)$ is irreducible over $\kappa$, then for any $i \geq 1$ there is a unique irreducible factor $h(x)$ of $\Phi_{m,\sigma}(x)$ for which $h(x) \mid f(\sigma^i(x))$.*

*Proof.* Fix $i \geq 1$. If $\alpha$ is a root of $f(x)$, then $\sigma^{m-i}(\alpha)$ is a root of $f(\sigma^i(x))$, so the minimal polynomial $h(x)$ of $\sigma^{m-i}(\alpha)$ divides $\Phi_{m,\sigma}(x)$ and $f(\sigma^i(x))$. Suppose there are two distinct irreducible factors $h_1(x)$ and $h_2(x)$ of $\Phi_{m,\sigma}(x)$ which divide $f(\sigma^i(x))$. Let $\alpha_j$ be a root of $h_j(x)$ for $j = 1, 2$. Then the numbers $\sigma^i(\alpha_j)$, $j = 1, 2$, are both roots of $f(x)$, so that $\sigma^i(\alpha_1)$ and $\sigma^i(\alpha_2)$ are conjugate over $\kappa$. But then

$$\sigma^{m-i}(\sigma^i(\alpha_1)) = \alpha_1 \quad \text{and} \quad \sigma^{m-i}(\sigma^i(\alpha_2)) = \alpha_2$$

are conjugate over $\kappa$, which is impossible since $\alpha_1$ and $\alpha_2$ have distinct minimal polynomials. □

**Lemma 3.5.** *If $f$ is a primitive irreducible factor of $\Phi_{m,\sigma}(x)$, then $f$ belongs to a cycle in $G_\sigma$. If $\lambda(f)$ is the length of the smallest cycle containing $f$, then $n = \lambda(f)$ is the smallest integer $n$ for which $f(x) \mid f(\sigma^n(x))$, and $\lambda(f)$ divides $m$. Moreover, $m|\lambda(f)\deg f$* (cf. [**11**, Theorem 14b]).

*Proof.* Under the given assumptions the roots of $f$ are periodic points of $\sigma$ of primitive period $m$. Let $h_i(x)$ be the irreducible factor of $\Phi_{m,\sigma}(x)$ guaranteed by Lemma 3.4. We then have

$$h_i(\sigma(x))|f(\sigma^{i+1}(x)) \quad \text{and} \quad h_{i+1}(x)|f(\sigma^{i+1}(x)),$$

which implies that $h_{i+1}(x)$ is the unique irreducible factor of $\Phi_{m,\sigma}(x)$ dividing $h_i(\sigma(x))$. Thus $h_{i+1} \to h_i$. Now let $n$ be any integer for which $f(x) \mid f(\sigma^n(x))$. Then $h_n = f$, so that

$$f = h_n \to \cdots \to h_{k+1} \to h_k \to \cdots \to h_1 \to f$$

is a cycle of length $n$ containing $f$. Conversely, the proof of Lemma 3.3 shows that the existence of a cycle of length $n$ containing $f$ implies $f(x) \mid f(\sigma^n(x))$. Noting that $f(x)$ divides $f(\sigma^m(x))$, and that the length of the smallest cycle containing $f$ divides the length of any cycle that contains $f$, gives the stated characterization of $\lambda(f)$ and shows that $\lambda(f)$ divides $m$. The last assertion follows from the fact that $\lambda(f)\deg f$ is equal to the total number of roots of the polynomials in a minimal cycle with $f$ and that these roots fall into orbits of size $m$. □

If we denote the map induced by $\sigma$ on the vertices of $G_\sigma$ by $\hat{\sigma}$, then a polynomial $f$ in a cycle of length $n$ is a periodic point of $\hat{\sigma}$ of order $n$. Lemmas 2.1 and 3.1 show further that every irreducible polynomial over $\mathbf{F}_q$ is *connected* to a polynomial in some cycle of $G_\sigma$.

We now prove

**Theorem 3.6.** *Let $\sigma(x)$ be any nonconstant polynomial over the finite field $\mathbf{F}_q$. Then the induced map $\hat{\sigma}$ has infinitely many fixed* *points. Equivalently, there are infinitely many irreducible polynomials* $f(x)$ *over* $\mathbf{F}_q$ *for which* $f(x) \mid f(\sigma(x))$.

*Proof.* Consider the polynomials

$$g_r(x) = \sigma(x) - \phi^r(x) = \sigma(x) - x^{q^r}, \qquad r \geq 1,$$

where $\phi(x) = x^q$ is the Frobenius map. If $a$ is a root of $g_r$, then $\sigma(a) = \phi^r(a)$ implies that $\sigma(a)$ is a conjugate of $a$ over $\mathbf{F}_q$, so the minimal polynomial $f$ of $a$ over $\mathbf{F}_q$ is a fixed point of $\hat{\sigma}$ ($\sigma$ takes a root of $f$ to a root of $f$). We have to show that the polynomials $g_r$ have an infinite number of distinct irreducible factors over $\mathbf{F}_q$.

First, suppose that $\sigma(x)$ is not a $p$-th power, where $p$ is the characteristic of $\mathbf{F}_q$, so that $\sigma'(x)$ is not identically 0. Assume that there are only a finite number of irreducible polynomials, say $f_i$, $1 \leq i \leq k$, which divide any of the $g_r$. Let $e_i$ be the multiplicity of $f_i$ in $g_r$. Then the multiplicity of $f_i$ in the derivative $g_r'$ is at least $e_i - 1$. Since $g_r'(x) = \sigma'(x) \neq 0$, this gives that $e_i$ is bounded independent of $r$, for each $i$. But this is clearly impossible, since $\deg g_r \to \infty$ as $r \to \infty$.

If $\sigma(x)$ is a $p$-th power, write $\sigma(x) = \tau(x)^{p^i}$, where $\tau(x)$ is not a $p$-th power. Then apply the above argument to $\tau$ and the polynomials

$$h_r(x) = \tau(x) - x^{q^r p^{-i}}, \qquad \text{for } r \text{ sufficiently large},$$

to get infinitely many irreducible factors of $h_r$ as $r \to \infty$. Since $g_r(x) = h_r(x)^{p^i}$, the same holds for $g_r$, completing the proof. □

**Corollary.** *For any nonconstant polynomial* $\sigma(x)$ *in* $\mathbf{F}_q[x]$, *the graph* $G_\sigma$ *has an infinite number of connected components, and infinitely many cycles of length* 1.

In the remainder of this paper we will show that the graph $G_\sigma$ also has an infinite number of cycles with length $> 1$, for a certain family of polynomials (see (5)). We conjecture that this fact is also true of any nonconstant polynomial which is not an iterate of the Frobenius map.

**4. Periodic points as eigenvectors.** For the remainder of this paper, we restrict ourselves to a special class of polynomials, namely

$$\sigma(x) = x^q + ax, \qquad \text{with } a \neq 0 \text{ in } \mathbf{F}_q. \tag{5}$$

Denote the order of $a$ in the multiplicative group of $\mathbf{F}_q$ by $\operatorname{ord}(a)$.

**Lemma 4.1.** *Let $\sigma(x)$ be as in* (5)*. If $(m,q)=1$ and $\operatorname{ord}(a)$ divides $m$, then $\sigma^m(x)-x$ is a $q$-th power. If $(m,q)=1$ and $\operatorname{ord}(a)$ does not divide $m$, then $\sigma^m(x)-x$ has no multiple factors.*

*Proof.* To prove the first assertion, we use the equation $\sigma=\phi+a*1$, where 1 denotes the identity map, and the fact that the maps in this equation are linear:

$$\begin{aligned}\sigma^m(x)=(\phi+a*1)^m(x)&=\sum_{k=0}^{m}\binom{m}{k}a^{m-k}\phi^k(x)\\&=\sum_{k=0}^{m}\binom{m}{k}a^{m-k}x^{q^k}.\end{aligned}\tag{6}$$

By assumption, $a^m=1$ so that all the terms in $\sigma^m(x)-x$ are $q$-th powers, implying that $\sigma^m(x)-x$ is itself a $q$-th power.

If $\operatorname{ord}(a)$ does not divide $m$, then (6) shows that the polynomial $f(x)=\sigma^m(x)-x$ satisfies

$$f(x)=\sigma^m(x)-x=g(x)^q+(a^m-1)x$$

for some polynomial $g(x)$. Hence $f'(x)=a^m-1\neq 0$ is relatively prime to $f(x)$, which implies that $\sigma^m(x)-x$ has no multiple roots. □

The result of this lemma also holds, of course, for any additive map

$$\sigma(x)=\sum_i a_i x^{q^i}=\sum_i a_i\phi^i=f(\phi),$$

with $a=a_0$. (Also see [**10**], where "symbolic" polynomial $f(\phi)$ in $\phi$ are used to study additive maps over $\mathbf{F}_q$.)

Since $\sigma$ is a linear map on $\mathbf{F}_q$, so also is $\sigma^m$, for any $m$, and so any element $\alpha$ in $\mathbf{F}_q$ for which $\sigma^m(\alpha)=\alpha$ is an *eigenvector* of $\sigma^m$ corresponding to the eigenvalue 1. Thus we have

**Lemma 4.2** (cf. [**10**, Theorem 3.50]). *Let $\sigma(x)$ be as in* (5)*. The set of periodic points of $\sigma$ of order $m$ is the eigenspace of $\sigma^m$ on $\hat{\mathbf{F}}_q$*

*corresponding to the eigenvector* 1*. Thus the set of periodic points of order* $m$ *is a vector space over* $\mathbf{F}_q$*.*

This lemma is also valid for any additive map $\sigma$.

In order to exploit Lemma 4.2 we compute the characteristic polynomial of $\sigma$ on a given finite subfield $\mathbf{F}_{q^n}$ of $\hat{\mathbf{F}}_q$. As before, let $\phi(x) = x^q$ be the Frobenius map. On the field $\mathbf{F}_{q^n}$, $\phi$ satisfies the minimal polynomial $\phi^n - 1 = 0$, since

$$(\phi^n - 1)(x) = x^{q^n} - x,$$

and since any polynomial in $\phi$ of smaller degree than $n$ could not have $q^n$ distinct roots. Hence $x^n - 1$ is also the characteristic polynomial of $\phi$, and the eigenvalues of $\phi$ are the $n$-th roots of unity $\zeta_n$. Using $\sigma = \phi + a * 1$, it follows that $\sigma$ has characteristic equation $(x-a)^n - 1$ and eigenvalues $a + \zeta_n$. Therefore the iterate $\sigma^m$ of $\sigma$ has eigenvalues $(a + \zeta_n)^m$. This point implies the following lemma.

**Lemma 4.3.** *Let* $E_{m,n}$ *be the space of periodic points of* $\sigma$ (*given by* (5)) *of order* $m$ *in* $\mathbf{F}_{q^n}$*, i.e., the* 1*-eigenspace of the map* $\sigma^m$ *on* $\mathbf{F}_{q^n}$*. If* $(n,q) = 1$*, then* $\tau_{m,n} = \dim_{\mathbf{F}_q} E_{m,n}$ *equals the number of* $n$*-th roots of unity* $\zeta_n$ *for which* $(a + \zeta_n)^m = 1$*.*

*Proof.* If $(n,q) = 1$, the minimal polynomial of $\phi$ on $\mathbf{F}_{q^n}$ has distinct roots so $\phi, \sigma$ and $\sigma^m$ are diagonalizable linear maps on the field $\mathbf{F}_{q^n}$. Hence the multiplicity of 1 as an eigenvalue of $\sigma^m$ equals the dimension of its 1-eigenspace. The lemma now follows from the above discussion. □

*Notes.* 1. A similar result holds for any additive map $\sigma = f(\phi)$. In this case $\tau_{m,n}$ equals the number of $n$-th roots of unity $\zeta_n$ for which $f(\zeta_n)^m = 1$.

2. It is a curious fact that the eigenvalues of the linear operator $\sigma$ on $\mathbf{F}_{q^n}$ are not usually contained in $\mathbf{F}_{q^n}$. The reason for this is that a primitive $n$-th root of unity $\zeta_n$ has degree $d$ over $\mathbf{F}_q$, where $d$ is the order of $q$ modulo $n$ (see [**3, 7, 10**]). If $\zeta_n$ lies in $\mathbf{F}_{q^n}$, then $d$ divides $n$, so $q^n \equiv 1 \pmod{n}$. The last congruence is generally

false, for example, whenever $(n, \varphi(n)) = 1$ and $q \not\equiv 1 \pmod{n}$. Thus, we consider two fields in the proof of Theorem 4.4 below; the field $\mathbf{F}_{q^n}$ containing the appropriate eigenvectors of $\sigma^m$, and the field $\mathbf{F}_{q^d}$ containing the eigenvalues of $\sigma$.

In the next theorem we use Lemma 4.3 to locate a field which contains all the periodic points of order $m$, when $(m, q) = 1$.

**Theorem 4.4.** *Let $\sigma(x)$ be given by* (5). *Suppose $(m, q) = 1$ and $d$ is the order of $q$ modulo $m$. If $n = q^d - 1$, then all the periodic points of $\sigma$ of order $m$ lie in $\mathbf{F}_{q^n}$, and*

$$\tau_{m,q^d-1} = \dim_{\mathbf{F}_q} E_{m,q^d-1} = \begin{cases} m-1, & \textit{if } \operatorname{ord}(a)|m, \\ m, & \textit{otherwise.} \end{cases}$$

*Proof.* Since the $n$-th roots of unity $\zeta_n$ are exactly the nonzero elements of the field $\mathbf{F}_{q^d}$, it follows that the set $\{a + \zeta_n, \zeta_n \neq -a\}$ consists of all the nonzero elements of $\mathbf{F}_{q^d}$, excluding $a$. Since $m$ divides $n$, and the multiplicative group $\mathbf{F}_{q^d}^{\times}$ is cyclic, there are exactly $m-1$ numbers $\zeta_n$, for which $a+\zeta_n$ is an $m$-th root of unity, if $a$ is an $m$-th root of unity, and $m$ numbers $\zeta_n$ if $a$ is not an $m$-th root of unity. Lemma 4.3 implies that $\sigma$ has either $q^{m-1}$ or $q^m$ distinct periodic points of order $m$ in $\mathbf{F}_{q^n}$, respectively. In the first case the polynomial $\sigma^m(x) - x$ is a $q$-th power and has at most $q^{m-1}$ distinct roots by Lemma 4.1; in the second case $\sigma^m(x) - x$ has $q^m$ distinct roots. The above argument shows that all these periodic points are contained in $\mathbf{F}_{q^n}$ and proves the theorem. □

**Corollary 1.** *The degrees of the irreducible factors of $\Phi_{m,x^q+ax}$, for $(m, q) = 1$, divide $q^d - 1$, where $d$ is the order of $q$ modulo $m$.*

**Corollary 2.** *Let $\sigma(x)$ be given by* (5). *If $(m, q) = 1$ and* $\operatorname{ord}(a)$ *divides $m$, then $\sigma^m(x) - x = f(x)^q$, where $f(x)$ has distinct roots.*

**Corollary 3.** *If $a = 1$ and $\sigma(x) = x^q + x$, then $\Phi_{m,\sigma}(x)$ is a $q$-th power for every integer $m$ for which $(m, q) = 1$. For such $m$, all the roots of $\Phi_{m,\sigma}(x)$ are periodic points of primitive period $m$.*

*Proof.* The first assertion follows from Lemma 4.1 and (1). The second follows from this and Corollary 2, since any nonprimitive roots of $\Phi_{m,\sigma}(x)$ would have multiplicity higher than $q$ in $\sigma^m(x) - x$. □

We show next how to compute the number of roots of $\Phi_{m,\sigma}(x)$ of a given degree.

**Theorem 4.5.** *Let $\sigma$ be as in* (5), *and let $\nu_{m,n}$ denote the number of periodic points of $\sigma$ of primitive period $m$ and exact degree $n$ over $\mathbf{F}_q$. Then*

$$\nu_{m,n} = \sum_{d|m} \sum_{e|n} \mu\left(\frac{m}{d}\right) \mu\left(\frac{n}{e}\right) q^{\tau_{d,e}},$$

*where $\tau_{m,n} = \dim_{\mathbf{F}_q} E_{m,n}$ is the dimension of the* 1*-eigenspace of $\sigma^m$ on $\mathbf{F}_{q^n}$ (given by Lemma* 4.3 *for $(n, q) = 1$).*

*Proof.* Since $\tau_{m,n}$ is the dimension of the space of all periodic points of order $m$ contained in $\mathbf{F}_{q^n}$, counting the elements of this space by primitive order and degree gives

$$q^{\tau_{m,n}} = \sum_{d|m} \sum_{e|n} \nu_{d,e}.$$

Applying Möbius inversion twice to this formula gives first that

$$\sum_{e|n} \nu_{m,e} = \sum_{d|m} \mu\left(\frac{m}{d}\right) q^{\tau_{d,n}}$$

and then that

$$\nu_{m,n} = \sum_{e|n} \mu\left(\frac{n}{e}\right) \sum_{d|m} \mu\left(\frac{m}{d}\right) q^{\tau_{d,e}},$$

which is the formula of the theorem.

**5. Special results for $\sigma(x) = x^2 + x$.** Before continuing our study of the factorization of $\Phi_{m,\sigma}(x)$ for $\sigma$ as in (5), we prove several results for the map $\sigma(x) = x^2 + x$ over $\mathbf{F}_2$. This map has some special properties not shared by the maps in odd characteristic.

**Theorem 5.1.** *If $p = 2^l - 1$ is a Mersenne prime, then $\Phi_{p,x^2+x}(x)$ is the product of $(2^{p-1} - 1)/p$ irreducible factors of degree $p$.*

*Proof.* We show that all the $p$-th order periodic points have degree $p$. The dimension of the 1-eigenspace of $\sigma^p$ on $\mathbf{F}_{2^p}$ is just $2^l - 2 = p - 1$, since for all eigenvalues $\zeta_p \neq 1$, $1 + \zeta_p$ has order $p$. This follows from

$$(1+\zeta_p)^p = (1+\zeta_p)^{2^l-1} = \frac{(1+\zeta_p)^{2^l}}{1+\zeta_p} = \frac{1+\zeta_p^{2^l}}{1+\zeta_p} = \frac{1+\zeta_p}{1+\zeta_p} = 1$$

and the fact that $p$ is prime. Noting that $\Phi_{p,x^2+x}(x)$ has exactly $2^{p-1}-1$ distinct roots (Corollary 3 to Theorem 4.4), and that the only $p$-th order periodic point of degree 1 is 0, it follows from Theorem 4.5 that $\nu_{p,p} = 2^{p-1} - 1$, hence all the primitive $p$-th order periodic points of $\sigma$ have degree $p$. □

The following converse to this theorem also holds.

**Theorem 5.2.** *If $p$ is a prime for which $\Phi_{p,x^2+x}(x)$ factors into irreducibles of degree $p$, then $p$ is a Mersenne prime.*

*Proof.* If $\Phi_{p,x^2+x}(x)$ factors in the given way over $\mathbf{F}_2$, then $\tau_{p,p} = p-1$, so that for every $p$-th root of unity $\zeta_p \neq 1$, $1 + \zeta_p$ has order $p$. If this is the case, it is not hard to see that the set $F$ of $p$-th roots of unity, together with 0, forms a field. For, if $\zeta_p$ and $\zeta_p'$ are arbitrary $p$-th roots of 1, we have

$$\zeta_p + \zeta_{p'} = \begin{cases} 0, & \text{if } \zeta_p = \zeta_{p'}, \\ \zeta_p(1 + \zeta_{p'}\zeta_p^{-1}) = \zeta_{p''}, & \text{otherwise.} \end{cases}$$

Since the product of $p$-th roots of unity is obviously a $p$-th root of unity, this proves the claim that $F$ is a field. But the characteristic of $F$ is 2 and $F$ has $p + 1$ elements, so we get that $p + 1 = 2^n$ for some $n$, i.e., $p$ is a Mersenne prime. □

By way of illustrating the last two results, note that the third diagram in Section 3 gives 7 of the 9 irreducible factors of $\Phi_{7,x^2+x}(x)$.

This raises the following question: are any of the factors of $\Phi_{p,x^2+x}(x)$ fixed points of $\hat{\sigma}$? If $f$ is an irreducible factor of $\Phi_{p,x^2+x}(x)$ which is not a fixed point of $\hat{\sigma}$, then $f$ must be in a cycle of length $p$ (by Lemma 3.5). If none of the factors of $\Phi_{p,x^2+x}(x)$ are fixed points, then the number of factors, $(2^{p-1}-1)/p$ must be divisible by $p$. We examine this quotient, the so-called Fermat quotient, mod$p$.

First, since $p-1 = 2^l - 2$ is divisible by $l$ (Fermat's theorem), we may write $p-1 = kl$, $k \neq 0$. Then we find, since $2^l \equiv 1 \pmod{p}$, that

$$(7) \quad \frac{2^{p-1}-1}{p} = \frac{2^{kl}-1}{2^l-1} = ((2^l)^{k-1} + (2^l)^{k-2} + \cdots + 1) \equiv k \pmod{p}.$$

This proves

**Theorem 5.3.** *For a Mersenne prime $p = 2^l - 1$,*

$$\frac{2^{p-1}-1}{p} \equiv \frac{p-1}{l} \pmod{p}.$$

Since $(p-1)/l$ is clearly not divisible by $p$, Theorem 5.3 shows that the Fermat quotient is never divisible by $p$ if $p$ is a Mersenne prime. In fact, there are only two known primes for which the Fermat quotient $(2^{p-1}-1)/p$ is divisible by $p$, namely, $p = 1093$ and $p = 3511$. See [**2**] for more on this question.

By Theorem 5.3 at least $(p-1)/l$ factors of $\Phi_{p,x^2+x}(x)$ cannot lie in cycles of length $p$, so we have the following consequence.

**Theorem 5.4.** *If $p = 2^l - 1$ is a Mersenne prime, then $\Phi_{p,x^2+x}(x)$ has at least $(p-1)/l$ factors of degree $p$ which are fixed points of $\hat{\sigma}$.*

**6. The factorization of $\Phi_{m,\sigma}$ for $(m,q) = 1$.** In this section we will show that for any $\sigma$ of the form $\sigma(x) = x^q + ax$, with $a \neq 0$ in $\mathbf{F}_q$, the induced map $\hat{\sigma}$ has infinitely many periodic points with period greater than 1. To prepare for this we study the factorization of $\Phi_{m,\sigma}$ in some detail.

For $d \geq 1$, let $P_d = \{\text{primitive divisors of } q^d - 1\}$, so that $P_d$ contains exactly the positive integers which divide $q^d-1$ but do not divide $q^k-1$ for $k < d$. To prove the following result concerning the irreducible factors of $\Phi_{m,\sigma}$, we require a lemma.

**Lemma 6.1.** *Let $\sigma(x) = x^q + ax$, where $a$ is a nonzero element of $\mathbf{F}_q$. Let $f$ be an imprimitive irreducible factor of $\Phi_{m,\sigma}(x)$, for some $m$ with $(m,q) = 1$. Then there is a unique $r < m$ with $(r,q) = 1$ for which $f$ divides $\Phi_{r,\sigma}(x)$ and for this $r$ we have $m = l.c.m.[r, \operatorname{ord}(a)]$. The exact power of $f$ dividing $\Phi_{m,\sigma}(x)$ is $f(x)^{q-1}$.*

*Proof.* Since $f$ is imprimitive, $f$ is certainly a primitive divisor of $\Phi_{r,\sigma}(x)$ for some $r \mid m$. There cannot be an additional $s < m$ with $(s,q) = 1$ for which $f \mid \Phi_{s,\sigma}(x)$. If there were, then $r < s$, and $f$ would have to be a multiple factor of $\Phi_{s,\sigma}(x)$, by [**11**, Theorem 1c]; this would imply, by the same result [**11**, Theorem 1d] that $f$ could not be a factor of $\Phi_{m,\sigma}(x)$. For the same reason $f$ cannot be a multiple factor of $\Phi_{r,\sigma}(x)$ and must be a multiple factor of $\Phi_{m,\sigma}(x)$. It follows from Corollary 2 to Theorem 4.4 and the equation

$$\sigma^m(x) - x = \Phi_{r,\sigma}(x)\Phi_{m,\sigma}(x) \prod_{d \mid m, d \neq r,m} \Phi_{d,\sigma}(x) \tag{8}$$

that the exact power of $f$ dividing $\Phi_{m,\sigma}(x)$ must be the $(q-1)$-st power. Furthermore, Lemma 4.1 shows that $\sigma^m(x) - x$ has multiple roots (and is then a $q$-th power) if and only if $\operatorname{ord}(a) \mid m$. Thus we get that $m$ is a multiple of $\lambda = \text{l.c.m.}[r, \operatorname{ord}(a)]$. Finally, (8), with $\lambda$ in place of $m$, shows that $f$ is a multiple factor of $\Phi_{\lambda,\sigma}(x)$, and the above argument implies $m = \lambda$. □

*Note.* If $q = 2$ there are no imprimitive factors of $\Phi_{m,x^2+x}(x)$; see Corollary 3 to Theorem 4.4.

**Theorem 6.2.** *Let $\sigma(x) = x^q + ax$, where $a \in \mathbf{F}_q$, $a \neq 0$. If $(m,q) = 1$ and $d$ is the order of $q$ modulo $m$, then the degrees of the irreducible factors of $\Phi_{m,\sigma}(x)$ are all primitive divisors of $n = q^d - 1$. In other words, if $m$ is in $P_d$, then the degrees of the irreducible factors of $\Phi_{m,\sigma}(x)$ are also in $P_d$. Moreover, the set of irreducible polynomials* *over* $\mathbf{F}_q$ *whose degrees are in the set* $P_d$ *coincides with the set of irreducible factors of* $\Phi_{m,\sigma}(x)$ *and of* $\Phi_{m,\sigma}(\sigma(x))$, *for* $m$ *in* $P_d$.

*Remark.* This says that all irreducibles over $\mathbf{F}_q$ of degree $\delta$, where $\delta$ is in $P_d$, belong to a cycle in the graph $G_\sigma$ or are 1-step connected to a polynomial in such a cycle.

*Proof.* By Theorem 4.4 the periodic points of $\sigma$ of order $m$ lie in $\mathbf{F}_{q^n}$. This shows that the degrees of the irreducible factors of $\Phi_{m,\sigma}(x)$ divide $n$.

We start by proving the assertions of the theorem for $d = 1$. By Theorem 4.4, the periodic points of $\sigma$ of order $q-1$ have degree dividing $q-1$, and the dimension of the space of periodic points of order $q-1$ equals $q-2$. On the other hand, the total number of elements of degree dividing $q-1$ over $\mathbf{F}_q$ equals $q^{q-1} = q * q^{q-2}$. Thus, we need to show that the other $(q-1)q^{q-2}$ elements of degree $q-1$ are roots of polynomials at level 1 in $G_\sigma$, i.e., are roots of

$$\prod_{d|q-1} \Phi_{d,\sigma}(\sigma(x)) = \sigma^{q-1}(\sigma(x)) - \sigma(x) \qquad (9)$$

$$= \sigma^q(x) - \sigma(x).$$

However, $\sigma^q(x) - \sigma(x) = (\phi + a)^q(x) - (\phi + a)(x) = x^{q^q} - x^q = (x^{q^{q-1}} - x)^q$, which has exactly the elements of the field $\mathbf{F}_{q^{q-1}}$ as roots. This proves all the assertions of the theorem for $d = 1$.

Now assume the assertion of the theorem is true for all integers less than $d$, and let $m$ be a primitive divisor of $q^d - 1$. Then the degree $\delta$ of an irreducible factor $f$ of $\Phi_{m,\sigma}(x)$ must divide $q^d - 1$. On the other hand, suppose that $\delta$ is a primitive divisor of $q^k - 1$ for $k < d$ so that $k \mid d$. Then $f$ is a factor of $\Phi_{r,\sigma}(x)$ or is 1-step connected to such a factor, for an integer $r$ in $P_k$, by the induction assumption. In the latter case, if $f$ is not a factor of $\Phi_{r,\sigma}(x)$ but is 1-step connected to such a factor, then its roots must be pre-periodic, contradicting the fact that the roots of $f$ are periodic points of $\sigma$. Hence $f$ is a factor of $\Phi_{r,\sigma}(x)$ for $r$ in $P_k$. This implies, since $P_k$ and $P_d$ are disjoint, that $f$ is a nonprimitive factor of $\Phi_{m,\sigma}(x)$. From Lemma 6.1, we conclude that $m = \text{l.c.m.}[r, \text{ord}\,(a)]$. However, $\text{ord}\,(a)$ divides $q-1$, so the order of $q \bmod m$ (namely, $d$) is the same as the order of $q \bmod r$ (namely, $k$), contradicting the fact that $k < d$. Hence, the degree of $f$ lies in $P_d$.

It remains to prove the last sentence of the theorem for the integer $d$. In analogy to (9), we have

$$\begin{aligned}\prod_{m|q^d-1} \Phi_{m,\sigma}(\sigma(x)) &= \sigma^{q^d-1}(\sigma(x)) - \sigma(x) \\ &= \sigma^{q^d}(x) - \sigma(x) \\ &= (x^{q^{q^d-1}} - x)^q.\end{aligned} \tag{10}$$

This shows that all the irreducible polynomials whose degrees lie in $P_d$ divide some $\Phi_{m,\sigma}(\sigma(x))$. Our induction assumption now implies that $m$ must also lie in $P_d$. To complete the proof of the theorem, we just note that any irreducible factor $g$ of $\Phi_{m,\sigma}(\sigma(x))$ which does not divide $\Phi_{m,\sigma}(x)$ is 1-step connected to an irreducible factor $f$ of $\Phi_{m,\sigma}(x)$. If $\deg f$ lies in $P_d$, then $\deg g$, as a multiple of $\deg f$, and as a divisor of $q^d - 1$ (by (10)), also lies in $P_d$. □

*Example.* We consider $q = 2$, $\sigma(x) = x^2 + x$, $P_6 = \{9, 21, 63\}$. We will use Theorem 4.5 to compute the degrees of the factors of $\Phi_{9,x^2+x}$, $\Phi_{21,x^2+x}$, and $\Phi_{63,x^2+x}$. We first make a table of the values of $\tau_{m,n} = \dim_{\mathbf{F}_q} E_{m,n}$ for divisors $m$ and $n$ of 63, where $E_{m,n}$, as in Section 4, denotes the vector space of periodic points of order $m$ lying in $\mathbf{F}_{q^n}$.

TABLE 1. Values of $\tau_{m,n}$

| $m/n$ | 1 | 3 | 7 | 9 | 21 | 63 |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 0 | 2 | 0 | 2 | 2 | 2 |
| 7 | 0 | 0 | 6 | 0 | 6 | 6 |
| 9 | 0 | 2 | 0 | 2 | 2 | 8 |
| 21 | 0 | 2 | 6 | 2 | 8 | 20 |
| 63 | 0 | 2 | 6 | 8 | 20 | 62 |

The values in this table were computed by finding the order of $(1+x)$ modulo each of the irreducible factors $f(x)$ of the polynomial $x^n - 1$ and counting how many of these orders divide $m$. This can be computed for all the factors at once by computing $(1+x)^d - 1 \pmod{x^n - 1}$ for divisors $d$ of 63 and determining which of the factors of $x^n - 1$ divide the residue. From this table and the formula of Theorem 4.5, we get

$$\nu_{9,9} = 0, \quad \nu_{9,21} = 0, \quad \text{and} \quad \nu_{9,63} = 252,$$

so that $\Phi_{9,x^2+x}$ splits into 4 factors of degree 63. In the same way,

$$\nu_{21,9} = 0, \quad \nu_{21,21} = 189, \quad \nu_{21,63} = 2^{20} - 2^8,$$
$$\nu_{63,9} = 252, \quad \nu_{63,21} = 2^{20} - 2^8, \quad \nu_{21,63} = 2^{62} - 2^{20} - 2^8 + 2^2.$$

Hence $\Phi_{21,x^2+x}$ factors as a product of 9 factors of degree 21 and 16640 factors of degree 63, while $\Phi_{63,x^2+x}$ factors into a product of 28 polynomials of degree 9, 49920 factors of degree 21, and $(1/63)(2^{62} - 2^{20} - 2^8 + 2^2)$ factors of degree 63.

The following table gives the degrees of irreducible factors of $\Phi_{m,x^2+x}(x)$ over $\mathbf{F}_2$, grouped by primitive divisors of $2^d - 1$, for $2 \le d \le 9$.

| $d$ | $m$ | degrees of irreducible factors of $\Phi_{m,x^2+x}(x)$ |
|---|---|---|
| 2 | 3 | 3 |
| 3 | 7 | 7 |
| 4 | 5 | 15 |
| | 15 | 5,15 |
| 5 | 31 | 31 |
| 6 | 9 | 63 |
| | 21 | 21,63 |
| | 63 | 9,21,63 |
| 7 | 127 | 127 |
| 8 | 17 | 85,255 |
| | 85 | 17,51,85,255 |
| | 51 | 85,255 |
| | 255 | 17,51,85,255 |
| 9 | 73 | 73,511 |
| | 511 | 73,511 |

The reader cannot have failed to notice the symmetry in this table or in the above computation. In fact, the following reciprocity theorem holds.

**Theorem 6.3 (Reciprocity Theorem).** *For any integers $m$ and $n$ prime to $q$, let $\tau_{m,n}(a) = \dim_{\mathbf{F}_q} E_{m,n}$ (corresponding to the map $\sigma(x) = x^q + ax$) and let $\nu_{m,n}(a)$ denote the number of distinct roots of $\Phi_{m,x^q+ax}(x)$ which have degree $n$ over $\mathbf{F}_q$. Then we have*

$$\tau_{m,n}(a) = \tau_{n,m}(-a) \quad \text{and} \quad \nu_{m,n}(a) = \nu_{n,m}(-a).$$

*In other words, the number of distinct roots of $\Phi_{m,x^q+ax}(x)$ of degree $n$ equals the number of roots of $\Phi_{n,x^q-ax}(x)$ of degree $m$.*

*Proof.* By Lemma 4.3, $\tau_{m,n}(a)$ equals the number of $n$-th roots of unity $\zeta_n$ for which

$$\zeta_n + a = \zeta_m \tag{11}$$

is an $m$-th root of unity. But this equation gives a one-to-one correspondence between the $\zeta_n$'s for which (11) holds and the $\zeta_m$'s for which

$$\zeta_m - a = \zeta_n.$$

This proves that $\tau_{m,n}(a) = \tau_{n,m}(-a)$. Now $\nu_{m,n}(a) = \nu_{n,m}(-a)$ follows easily from Theorem 4.5. □

**Corollary.** *If $q = 2^r$ and $a$ lies in $\mathbf{F}_q$, then for any odd integers $m$ and $n$, the number of distinct roots of $\Phi_{m,x^q+ax}(x)$ of degree $n$ over $\mathbf{F}_q$ equals the number of distinct roots of $\Phi_{n,x^q+ax}(x)$ of degree $m$ over $\mathbf{F}_q$.*

Using this corollary we can show that there are infinitely many irreducible polynomials over $\mathbf{F}_2$ which lie in cycles of $G_\sigma$ of length $> 1$. For example, let $p$ be a prime which is not a Mersenne prime. Theorem 5.2 shows that $\Phi_{p,x^2+x}(x)$ has an irreducible factor of degree $m \neq p$, where $m$ and $p$ both lie in $P_d$ for some $d \neq 1$. By the above corollary, $\Phi_{m,x^2+x}(x)$ has an irreducible factor $f$ of degree $p$. If $f$ were a fixed point of $\hat{\sigma}$, then its roots would consist of complete orbits under $\sigma(x) = x^2 + x$, and its degree would have to be divisible by $m$, $m$

being the size of the orbits. But $m$ cannot divide $p$, unless $m = 1$; however, 1 and $p$ don't lie in the same set $P_d$. Thus, $f$ lies in a cycle of length $\lambda > 1$, where $\lambda$ divides $m$ (Lemma 3.5). This shows that the induced mapping $\hat{\sigma}$ has infinitely many periodic points which are not fixed points.

In order to generalize this argument we prove the following result related to Theorem 5.2. Let $p = \text{char}\, \mathbf{F}_q$.

**Lemma 6.4.** *If $a \neq 0$ lies in $\mathbf{F}_q$ and $l$ is an odd prime number which does not divide $q(q-1)$, and which is not a prime of the form $(p^n - 1)/(p-1)$, then not all of the irreducible factors of $\Phi_{l,x^q+ax}(x)$ can have degree $l$.*

*Proof.* Suppose instead that all of the irreducible factors of $\Phi_{l,x^q+ax}(x)$ do have degree $l$. Then all of these factors are primitive since the factors of

$$\Phi_{1,x^q+ax}(x) = x(x^{q-1} + a - 1)$$

have degrees dividing $q-1$ by Theorem 6.2. Furthermore, it is clear that the only root of $\Phi_{1,\sigma}(x)$ in $\mathbf{F}_{q^l}$ is the root 0, since the factor of degree $q-1$ has no nonzero roots in $\mathbf{F}_q$. Note that $\deg \Phi_{l,\sigma}(x) = q^l - q$. There are two cases to consider.

*Case* i). If $a = 1$, then $\Phi_{l,\sigma}(x)$ is a $q$-th power, by Corollary 3 to Theorem 4.4. It follows that $|E_{l,l}| = q^{l-1}$, whence the dimension of $E_{l,l}$ must be $l-1$. Thus, by Lemma 4.3, for every $l$-th root of unity $\zeta \neq 1$, $\zeta + 1$ is also an $l$-th root of unity (this because 2 has order dividing $q-1$ if $q$ is odd). It follows as in Theorem 5.2, that the set of $(p-1)l$-th roots of unity, together with 0, forms a field. Therefore, $(p-1)l + 1 = p^n$, and hence $l = (p^n - 1)/(p-1)$, which is excluded by hypothesis.

*Case* ii). If $a \neq 1$, then $l$ does not divide the order of $a$, so Lemma 4.1 implies that $\Phi_{l,\sigma}(x)$ has distinct roots. Hence these roots, together with 0, form a vector space over $\mathbf{F}_q$, implying that $q^l - q + 1 = q^n$ for some $n \geq 1$, clearly an impossible equation.

This proves the lemma. □

**Theorem 6.5.** *Let $\sigma(x) = x^q + ax$, where $a \neq 0$ is an element of $\mathbf{F}_q$.*

*If $l$ is an odd prime which does not divide $q(q-1)$ ($q$ odd) and which is not a prime of the form $(p^n-1)/(p-1)$, then there is an irreducible polynomial $f$ of degree $l$ which lies in a cycle in $G_\sigma$ of length $\lambda > 1$, where $\lambda \mid q^d - 1$ and $d$ is the order of $q$ modulo $l$. Thus, $\lambda$ is a period of $\hat{\sigma}$.*

*Proof.* By Lemma 6.4, $\Phi_{l,x^q-ax}(x)$ has a factor of degree $m \neq l$, where $m$ lies in $P_d$, and $d > 1$. The reciprocity theorem implies that $\Phi_{m,x^q+ax}(x)$ has a factor $f$ of degree $l$. If $f$ were a fixed point of $\hat{\sigma}$, then its roots would fall into orbits of length $m$, impossible since $m$ does not divide $l$ ($m \neq 1$ since $d > 1$). Hence $f$ lies in a cycle of length $\lambda$, where $\lambda \mid m$ and $m \mid \lambda l$ (Lemma 3.5). The last fact implies that either $\lambda = m$ or $l \mid m$ and $\lambda = m/l$. □

**Corollary 1.** *The induced map $\hat{\sigma}$ of $\sigma(x) = x^q + ax$ ($a \neq 0$ in $\mathbf{F}_q$) has infinitely many periodic points which are not fixed points.*

**Corollary 2.** *The induced map $\hat{\sigma}$ of $\sigma(x) = x^2 + x$ (over $\mathbf{F}_2$) has infinitely many periods which are relatively prime to each other and to 2.*

*Proof.* Take $d_i > 6$ to be an infinite sequence of pairwise relatively prime, odd composite integers, for $i \geq 1$. By Bang's theorem (see [**12**, page 27]), the integers $2^{d_i} - 1$ each have a primitive prime divisor $l_i$ (which cannot be a Mersenne prime by the assumption on $d_i$). The theorem implies that there is an irreducible polynomial $f_i$ of degree $l_i$ which is a periodic point of $\hat{\sigma}$ of order $\lambda_i$, where $\lambda_i$ divides $2^{d_i} - 1$. Since the integers $d_i$ are pairwise relatively prime, and since $(2^{d_i} - 1, 2^{d_j} - 1) = 1$ if $i \neq j$, the same is true of the $\lambda_i$. □

Corollary 2 is probably true for the more general maps $\sigma(x) = x^q + ax$ also, but the proof breaks down at the last step. In place of $(2^{d_i} - 1, 2^{d_j} - 1) = 1$, we have instead $(q^{d_i} - 1, q^{d_j} - 1) = q - 1$, and it is possible, though not likely, for all but finitely many of the $\lambda_i$ to divide $q - 1$. By the last assertion in the proof of Theorem 6.5, this would imply that $m_i = \lambda_i l_i$ for all large $i$, since the equality $m_i = \lambda_i$ would imply that $\lambda_i$ is a primitive divisor of $q^{d_i} - 1$ and therefore not a divisor of $q-1$.

**7. Periodic points of primitive order $p^k m$.** Up to now we have focused on the iterates of $\sigma$ of order $m$ prime to $p$, the characteristic of the ground field. We conclude this part by using Theorems 4.4 and 6.2 to prove several results about the factors of $\Phi_{mp^k,\sigma}(x)$, where $(m,p)=1$. For the whole section we assume $\sigma$ has the form (5).

**Theorem 7.1.** *If $(m,p)=1$, the degrees of the irreducible factors of $\Phi_{mp^k,\sigma}(x)$ divide $p^k(q^{p^k d}-1)$, where $d$ is the order of $q^{p^k}$ modulo $m$. All the primitive irreducible factors of $\Phi_{mp^k,\sigma}(x)$ have degrees of the form $p^k\delta$, where $\delta$ divides $(q^{p^k d}-1)$.*

*Proof.* We use the fact that $\Phi_{mp^k,\sigma}(x)$ divides $\Phi_{m,\sigma^{p^k}}(x)$, by the formula (see [**11**, Lemma 4])

$$\Phi_{m,\sigma^{p^k}}(x)=\prod_{i=0}^{k}\Phi_{mp^i,\sigma}(x). \tag{12}$$

By Theorem 4.4, applied to the map $\sigma^{p^k}(x)=x^{q^{p^k}}+a^{p^k}x$ over $\mathbf{F}_{q^{p^k}}$, the degrees of the irreducible factors of $\Phi_{m,\sigma^{p^k}}(x)$ over the field $\mathbf{F}_{q^{p^k}}$ divide $q^{p^k d}-1$, where $d$ is the order of $q^{p^k} \pmod m$. The first assertion of the theorem follows immediately.

Now fix a $k\geq 0$. By Theorem 6.2, all the irreducible polynomials over $\mathbf{F}_{q^{p^k}}$ of degree $m$, where $m$ is a primitive divisor of $q^{p^k d}-1$, divide $\Phi_{n,\sigma^{p^k}}(x)$ or $\Phi_{n,\sigma^{p^k}}(\sigma^{p^k}(x))$, where $n$ is also a primitive divisor of $q^{p^k d}-1$. Hence the elements $\beta$ whose degrees over $\mathbf{F}_{q^{p^k}}$ are $m$ are either periodic points of period dividing $np^k$ or are pre-periodic points of $\sigma$.

It follows that if $\beta$ is a primitive root of $\Phi_{mp^k,\sigma}(x)$, its degree over $\mathbf{F}_q$ must be divisible by $p^k$. Suppose instead that this degree equals $\delta p^i$ for $i<k$ and $\delta$ prime to $p$. Then for some $e$, $\delta$ is a primitive divisor of $q^{p^i e}-1$, and the comments above imply $\beta$ is either a pre-periodic point of $\sigma$ or that $\beta$ has period $np^i$, where $n$ divides $q^{p^i e}-1$. But both situations are impossible since $\beta$ has primitive period $mp^k$. this completes the proof. $\square$

In the following result we exhibit roots of some of the primitive irreducible factors of $\Phi_{mp^k,\sigma}(x)$. The result depends on the fact that $\sigma^{p^k}$ is a linear map over the field $\mathbf{F}_{q^{p^k}}$.

**Theorem 7.2.** *Let $\alpha \neq 0$ be a primitive root of $\Phi_{m,\sigma}(x)$ for the map $\sigma(x) = x^q + ax$, where $(m,p) = 1$, and let $\lambda$ have degree $p^k$ over $\mathbf{F}_q$. Then $\lambda\alpha$ is a primitive root of $\Phi_{mp^k,\sigma}(x)$ and* $\deg(\lambda\alpha) = p^k \deg \alpha$.

*Proof.* We have $\sigma^m(\alpha) = \alpha$. Furthermore, $\sigma^{p^k}(\lambda\alpha) = \lambda\sigma^{p^k}(\alpha)$, so that $\sigma^{mp^k}(\lambda\alpha) = (\sigma^{p^k})^m(\lambda\alpha) = \lambda\sigma^{mp^k}(\alpha) = \lambda\alpha$. In the same way, $\sigma^{rp^k}(\lambda\alpha) = \lambda\sigma^{rp^k}(\alpha) = \lambda\alpha$ if and only if $m$ divides $rp^k$, which holds if and only if $m$ divides $r$. Thus, $\lambda\alpha$ is a primitive root of $\Phi_{m,\sigma^{p^k}}(x)$. We need to show that $\lambda\alpha$ is a root of the factor $\Phi_{mp^k,\sigma}(x)$ in (12).

To show this we compute the degree of $\lambda\alpha$. Suppose that $\deg(\lambda\alpha) = r$. Then $r$ is the least integer for which $\lambda\alpha$ satisfies $(\lambda\alpha)^{q^r} = \lambda\alpha$. The last equation is equivalent to $(\lambda)^{q^r-1} = (1/\alpha)^{q^r-1}$, which in turn implies that both $(\lambda)^{q^r-1}$ and $(\alpha)^{q^r-1}$ lie in $\mathbf{F}_q$, since $\alpha$ and $\lambda$ have relatively prime degrees over $\mathbf{F}_q$. Thus, by a standard argument, $\lambda^{q^r} = b\lambda$ for some $b$ in $\mathbf{F}_q$, which gives $\lambda^{q^{ir}} = b^i\lambda$ and therefore $\lambda = \lambda^{q^{p^k r}} = b^{p^k}\lambda$, whence $b^{p^k} = 1$ and $b = 1$. Thus, $\lambda^{q^r} = \lambda$ and $\alpha^{q^r} = \alpha$, giving that $r$ is divisible both by $\deg \alpha$ and $\deg \lambda$. Hence, $r = \deg(\lambda\alpha) = \deg(\lambda)\deg(\alpha) = p^k \deg(\alpha)$.

Thus, $p^k$ divides the degree of $\lambda\alpha$, which implies by Theorem 7.1 that $\lambda\alpha$ can't be a root of $\Phi_{rp^i,\sigma}(x)$ for $i < k$ and any $r$ prime to $p$. It follows from (12) and the argument in the first part of the proof that $\lambda\alpha$ is a primitive root of $\Phi_{mp^k,\sigma}(x)$. □

*Example.* A root $\alpha$ of $x^3 + x + 1 = 0$ over $\mathbf{F}_2$ is a periodic point of $\sigma(x) = x^2 + x$ with primitive period 3. If $\lambda$ is a root of $x^2 + x + 1 = 0$ over $\mathbf{F}_2$, then $\lambda\alpha$ is a root of the sextic $x^6 + x^4 + x^2 + x + 1$. In fact,

$$\Phi_{3,\sigma}(x) = (x^3 + x + 1)^2$$

and

$$\Phi_{6,\sigma}(x) = (x^3 + x + 1)^2(x^6 + x^4 + x^2 + x + 1)^4(x^6 + x^3 + 1)^4,$$

so half of the primitive periodic points of period 6 arise from primitive third order periodic points by the construction of Theorem 7.2. The two irreducible sixth degree factors make up the cycle of length 2 in the diagrams of Section 3, so the other primitive periodic points of period 6 are given by $\sigma(\lambda\alpha)$ as $\lambda$ and $\alpha$ vary.

**Acknowledgment.** We are grateful to D. Thakur and F. Vivaldi for several useful conversations and their remarks concerning an earlier version of this paper.

## REFERENCES

**1.** A.F. Beardon, *Iteration of rational functions*, Springer Grad. Texts Math. **132**, Springer-Verlag, 1991.

**2.** J. Brillhart, J. Tonascia and P. Weinberger, *On the Fermat quotient*, Computers in Number Theory, Academic Press, 1971, 213–222.

**3.** L. Carlitz, *Single variable Bell polynomials*, Seminario Matematico de Barcelona, Collectanea Mathematica **14** (1962), 3–25.

**4.** ———, *A class of polynomials*, Trans. Amer. Math. Soc. **43** (1938), 167–182.

**5.** R.M. Corless, *Continued fractions and chaos*, Amer. Math. Monthly **99** (1992), 203–215.

**6.** R.L. Devaney, *An introduction to chaotic dynamical systems*, Addison-Wesley, Reading, 1987.

**7.** W.J. Guerrier, *The factorization of the cyclotomic polynomials* mod$p$, Amer. Math. Monthly **75** (1968), 46.

**8.** D.R. Hayes, *Explicit class field theory for rational function fields*, Trans. Amer. Math. Soc. **189** (1974), 77–91.

**9.** J.C. Lagarias, *Number theory and dynamical systems*, AT&T Bell Laboratories, 1991.

**10.** R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and Its Applications, vol. 20, Addison-Wesley Publ. Co., Reading, 1983.

**11.** P. Morton and P. Patel, *The Galois theory of periodic points of polynomial maps*, Wellesley College, 1992.

**12.** P. Ribenboim, *The little book of big primes*, Springer-Verlag, New York, 1991.

**13.** B.L. van der Waerden, *Algebra*, vol. 1, Frederick Ungar Publishing Co., 1971.

**14.** F. Vivaldi, *Geometry of linear maps over finite fields*, Nonlinearity **5** (1992), 133–147.

**15.** ———, *Dynamics over irreducible polynomials*, Nonlinearity **5** (1992), 941–960.

**16.** F. Vivaldi and S. Hatjispyros, *Galois theory of periodic orbits of rational maps*, Nonlinearity **5** (1992), 961–978.

Department of Mathematics, University of Illinois at Urbana-Champaign, Urbana, Illinois 61801

Department of Mathematics, Wellesley College, Wellesley, MA 02181